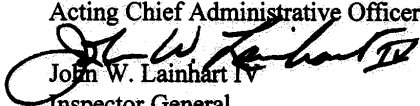


John W. Lainhart IV
Inspector General

Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990

MEMORANDUM

TO: Jeff Trandahl
Acting Chief Administrative Officer

FROM: 
John W. Lainhart IV
Inspector General

DATE: March 24, 1997

SUBJECT: Audit Report - Improvements Needed In The House's Contingency And Disaster Recovery Planning For Telecommunications (Report No. 97-CAO-07)

This is our final report on the audit of contingency and disaster recovery planning activities within the U.S. House of Representatives (House). This audit is the fourth of five audits performed on the House telecommunications environment. The objectives of this audit were to (1) prepare a limited HIR Telecommunications organization and operations profile and review for reasonableness, (2) determine if network backup and recovery can be achieved while minimizing loss of operations, (3) determine if emergency or contingency provisions have been incorporated into the major vendor contracts that support the House telecommunications network to ensure continuous vendor support is available and can be relied upon, and (4) determine if the backup and contingency plan in place is thorough and comprehensive to ensure that business interruption can be minimized in the case of a disaster. This audit also addresses the status of actions to correct shortcomings in telecommunications disaster recovery and contingency planning reported in our Calendar Year (CY) 1995 comprehensive audit of the House.

In this report, we identified contingency and disaster recovery planning weaknesses that may impair the House's ability to react to an unforeseen disaster and restore telecommunications service to users in a timely manner and made appropriate recommendations for corrective action. We also found that the majority of recommendations made to correct redundancy problems during the 1995 comprehensive House audit have not been fully implemented.

In response to our September 27, 1996 draft report, your office fully concurred with our findings, conclusions, and recommendations. The January 16, 1997 formal management response is incorporated into this final report and included in its entirety as an appendix.

We appreciate your office's positive attitude and cooperation throughout this audit. If you have any questions or require additional information regarding this report, please call me or David I. Berran at (202) 226-1250.

cc: Speaker of the House
Majority Leader of the House
Minority Leader of the House
Chairman, Committee on House Oversight
Ranking Minority Member, Committee on House Oversight
Members, Committee on House Oversight

IMPROVEMENTS NEEDED IN THE HOUSE'S CONTINGENCY AND DISASTER RECOVERY PLANNING FOR TELECOMMUNICATIONS

*Report No. 97-CAO-07
March 24, 1997*

RESULTS IN BRIEF

CONCLUSIONS

Since the House infrastructure places a high degree of reliance on the ability to communicate, the logical course of action would be to implement an approved and workable telecommunications contingency/disaster recovery plan designed to counter any number of disasters/threats in order to restore and maintain that capability. However, our review indicated the Communications Group had not fully developed, completely documented, or tested an up-to-date, comprehensive contingency/disaster recovery plan. Without such a contingency/disaster recovery plan, HIR cannot ensure that Members, Committees, and other House offices would continue to have telecommunications services in the event of a disaster or that recovery would be timely and complete. The need to set a contingency plan in motion could occur at any time due to the potential threat of natural disaster, system or electrical failure resulting in some aspect of network failure, unintentional errors, terrorism, or other similar acts. Given the reactive nature/makeup of the existing plan, such unanticipated acts could seriously affect the House's ability to maintain telecommunication services and continue business as usual.

We also noted deficiencies concerning the lack of off-site storage and rotation for the Private Branch Exchange (PBX) and telecommunications system software backup tapes. Without an adequate off-site storage and rotation process, the House's ability to obtain backup data could be severely limited or restricted. As a result, the recovery process would not occur smoothly in order to minimize business interruption and reduce the risk of loss due to the unavailability of current data. In addition, the placement of the existing voice system architecture increases the vulnerability of outages for major portions of telephone service at the House. All four PBX platforms serving House Members and staff are located in the Longworth building switch room. Because of the centralized placement of these PBX platforms, there is a greater potential for a single event (mechanical, natural or man-made disaster) to disrupt telephone service for all or a major portion of the House's telephone users.

We also noted conditions with regard to the current wiring infrastructure that are potentially hazardous and which, in our view, require management attention. Specifically, we found that cables are not adequately protected and telecommunications wire closets have potentially serious environmental and safety hazards. The wiring infrastructure throughout the House office buildings is one the most critical components of the House Telecommunications network. This infrastructure carries all voice, data, and video traffic. Correct installation and maintenance is crucial to maintaining the integrity of House telecommunications services.

Finally, we noted that the majority of recommendations made to correct redundancy problems during the 1995 comprehensive House audit have not been fully implemented. However, given the fact that we have already made recommendations concerning these serious telecommunications deficiencies; that corrective action is being taken; and that Communications Group officials have readily agreed to include

issues addressed in this section of the audit report in their business impact analysis, we are not making any formal recommendations with respect to these issues. However, we will conduct followup work as appropriate to determine what progress is being made and expect HIR management to routinely keep our office apprised of completed projects and any projects whose milestones need to be adjusted (as is currently being done).

RECOMMENDATIONS

The 14 recommendations we developed during this audit should, if properly implemented, improve the House's position with regard to telecommunications contingency planning and disaster recovery. Key recommendations include: (1) modifying the current Communications Contingency/Disaster Recovery Plan to encompass a detailed, proactive methodology that would encompass a distributed network topology and include it in the overall, House-wide plan; (2) utilizing the capabilities of software-based development tools (executed by in-house staff or contractor) that would best meet the needs of the House for comprehensive telecommunications contingency/disaster recovery planning; (3) developing and implementing routine procedures for off-site tape storage and retention of critical telecommunications software and data and incorporating these procedures into the official contingency/disaster recovery plan; (4) conducting a contingency-based risk assessment, including threat and vulnerability analyses, of the PBX platforms located in the Longworth building and using the results of the risk assessment to determine the appropriate course of action; and (5) modifying the current HIR House-wide contingency plan to add the PBX platforms and include them in cyclical testing.

Other recommendations involving wiring infrastructure include: (1) modifying the current telecommunications cleaning contract to include demarcation¹ rooms; (2) review procedures for monitoring contract compliance; (3) initiate deliberations with the Architect of the Capitol (AOC) regarding the feasibility of transferring responsibility for the demarcation rooms to the HIR Communications Group and evaluate points of responsibility governing access to these and all other rooms containing telecommunications equipment; (4) request the AOC to review procedures for monitoring temperature readings within the demarcation rooms; (5) conduct a risk assessment and/or benefit-cost analysis to determine the viability of adopting a diverse path protection scheme for voice services; and (6) develop Communications' policy that establishes rigid conduit as a de facto standard with justified exceptions made for the use of innerduct conduit.

MANAGEMENT RESPONSE

In the January 16, 1997 response to our draft report, the Acting Chief Administrative Officer (CAO) agreed with the findings and recommendations in this report, and indicated that corrective actions have been initiated for some areas and planned for the remaining areas. Specifically, the CAO will (1) seek the services of an experienced contractor to upgrade the current Contingency and Disaster Recovery plan for telecommunications; (2) conduct risk assessments on placement of the PBX platforms and the use of a diverse path protection scheme for voice services;

¹ A demarcation room is the area in a building in which the carrier facilities are handed off to the user organization. This location is the demarcation between the outside plant of the carrier, which is the carrier's responsibility, and the inside wiring of the building, which is the responsibility of the landlord/owner.

(3) modify tape backup and storage procedures for PBX and telecommunications system software; (4) modify the existing room cleaning contract to ensure coverage of all affected rooms; (5) negotiate with the Architect of the Capitol to (a) review procedures for monitoring temperature readings in demarcation rooms, (b) transfer responsibility for demarcation rooms to HIR Communications, and (c) review and develop/modify security procedures governing access to said rooms; and (6) ensure all telecommunications contingency and disaster recovery-related issues are included in the overall House-wide contingency/disaster recovery plan.

OFFICE OF INSPECTOR GENERAL COMMENTS

The CAO's planned actions are responsive to the issues we identified and, when fully implemented, should fully satisfy the intent of the recommendations.

[This page intentionally left blank]

TABLE OF CONTENTS

TRANSMITTAL MEMORANDUM

RESULTS IN BRIEF i

I. INTRODUCTION

Background 1

Objectives, Scope, And Methodology 2

Internal Controls 3

Prior Audit Coverage..... 3

II. FINDINGS AND RECOMMENDATIONS

Finding A: Comprehensive, Proactive Approach Needed To Bolster Contingency And
Disaster Recovery Planning..... 5

Finding B: Tape Backup Storage and Rotation Procedures Need To Be Improved..... 9

Finding C: Centralized PBX Platforms Place House-wide Telephone
Services At Risk 11

Finding D: Potential Hazards Could Be Eliminated With Improvements To The
Current Wiring Infrastructure 14

III. EXHIBIT

Status Of Implementation Of Prior Telecommunications
Audit Report Recommendations 18

IV. APPENDIX

CAO Management Response To The Draft Report

[This page intentionally left blank]

I. INTRODUCTION

Background

The Communications Group of House Information Resources (HIR) is responsible for the telecommunications needs of the House of Representatives (House). The Communications Group provides connectivity and manages networks for the House in Washington, D.C. and the Member district offices, providing access for all House organizations and entities (Members, Committees, House offices, and staff) to internal and external sources. The group provides and manages telephone and voice mail facilities, and supports video conferencing capabilities. Internet² connectivity is also administered by the Communications Group, facilitating Member and staff research and providing for dissemination of House information to the public. Its technical staff is responsible for evaluating and recommending commercially available voice and data equipment, designing integrated telecommunications solutions, developing specifications and procedures, and assisting in the implementation of these products. During the course of this review, the Committee on Appropriations, Subcommittee on Legislative, approved a FY 97 request of \$700,000 for telecommunications network contingency and disaster recovery improvements.

The Communications Group is composed of Voice and Video, Network Systems Engineering, Network Configuration Management, Network Installation and Maintenance, and Network Control Center (NCC³). The Voice and Video group provides ongoing operation and future planning for the House voice and video telecommunications systems. These systems include the nationwide network, the Washington, D.C. telephone system, the voice mail facilities, and group and desktop video capabilities. Furthermore, the Voice and Video group administers (1) upgrades of telephone switches, (2) contracts for telecommunications services, (3) classified secure telecommunications services, (4) the telecommunications accounting system, (5) emerging capabilities of computer telephony integration, and (6) the plant and equipment inventory. The Network Systems Engineering group prepares all engineering studies and testing to improve services and capacity on data networks serving the House as well as assisting in the analysis and troubleshooting of network problems and special project support that may lead to additional services provided to all clients. The Network Configuration Management group provides inventory, configuration, topology, and system maintenance support for all network hardware and software residing on the House data networks. Network support also includes network routers⁴, bridges⁵, repeaters⁶, and HUBs⁷ that comprise the House's infrastructure. Furthermore, the Network Configuration Management group provides the following services: Internet access, House mainframe access, local campus networking, district office networking, and domain name service. The Network Installation and Management group is responsible for the installation and troubleshooting of connections to House networks. Network Installation and Management also installs, maintains, and troubleshoots House telecommunication systems, including the House campus networks, Wide Area Network (WANs), and the House Systems Network Architecture⁸ network as well as resolving problems

² The Internet is a large international network that connects many computer systems, providing network services including, electronic mail (i.e., E-mail), remote terminal sessions, and multi-media services such as the world-wide web.

³ The Network Controller Center (NCC) manages the telecommunications network within the House.

⁴ A router is an intelligent hardware device in a network that routes messages between local area networks and wide area networks. Routers see the network as network addresses and all the possible paths between them. They read the network address in a transmitted message and can make decisions on how to send it based on the most expedient route (traffic load, line costs, speed, etc.).

⁵ A bridge is a functional unit that interconnects two local area networks that use the same logical link control protocol but may use different medium access control (MAC) protocols.

⁶ A repeater is a device used to amplify or reshape signals.

⁷ A HUB is a device where multiple workstations may connect to make up a network. This may be an active device, in which case, it functions as a concentrator or repeater.

⁸ The part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among users and provides protocols for controlling the resources of various network configurations.

with other House offices, vendors, and internal HIR staff. The NCC group performs the monitoring and controlling for the House network operations, which include the asynchronous dial-in network, the systems network architecture, the public data network, the House WANs, and the House campus networks. Major tasks include: network problem management, network performance monitoring, operational telephone support for network assistance, hardware and software diagnostics and recovery, and end-user network problem analysis.

Objectives, Scope, and Methodology

The objectives of this review were to (1) prepare a limited HIR Communications organization and operations profile and review for reasonableness, (2) determine if network backup and recovery can be achieved while minimizing loss of operations, (3) determine if emergency or contingency provisions have been incorporated into the major vendor contracts that support the House telecommunications network to ensure continuous vendor support is available and can be relied upon, and (4) determine if the backup and contingency plan in place is thorough and comprehensive to ensure that business interruption can be minimized in the case of a disaster. This audit also addressed the status of actions to correct shortcomings in telecommunications disaster recovery and contingency planning reported in our Calendar Year (CY) 1995 comprehensive audit of the House.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. The audit work included such evaluations and auditing procedures as were considered necessary under the circumstances. We conducted our audit work during the period July 1996 through August 1996 at HIR located in Washington, D.C.

In conducting this review, we performed the following specific tasks:

- Reviewed applicable government-wide internal control criteria that addresses controls in computer-based systems. Reviewed industry related documentation and reference materials that address telecommunications related issues, specifically contingency and disaster recovery planning.
- Interviewed HIR staff: Communications management, Security Manager, Enterprise Computing management; involved in telecommunications management, contingency and disaster recovery planning, and tape management.
- Evaluated the network topology for multiple telecommunications paths, backup, and off-site retention procedures for telecommunications software.
- Reviewed critical vendor contract specifications for coverage and support.
- Reviewed the current backup and contingency plan for minimizing business interruptions.
- Evaluated the follow-up actions performed as a result of the 1995 comprehensive audit of House operations for the backup of the NCC, the House-wide contingency and disaster recovery plan as it overlaps with the telecommunications contingency and disaster recovery plan, and telecommunications redundancy issues.

Internal Controls

During this review, we evaluated internal controls over the Communications Group's contingency and disaster recovery plan, and tape backup retention practices. We also reviewed existing vendor contracts to determine the existence of contingency provisions and completed followup work on redundancy weaknesses reported in the prior year's audit. The internal control weaknesses we identified are described in the "Findings and Recommendations" section of this report.

Prior Audit Coverage

House Computer Systems Were Vulnerable To Unauthorized Access, Modification, And Destruction (Report No. 95-CAO-18, dated July 18, 1995): This report was issued to address findings associated with a lack of adequate systems access controls within the House complex. We noted weaknesses concerning the lack of adequate systems access controls. This report identified improvements needed in: (1) disaster recovery planning and testing for HIR

operations, and (2) implementing and updating the business impact analysis identifying those business processes and systems that are critical to the business continuity of the organizations supported by HIR, as well as office-level systems and telecommunications links supporting Member, Committee, and other House office operations currently not addressed by the existing mainframe data center disaster recovery plan. This report also recommended the CAO: (3) evaluate backup and business recovery alternatives that would facilitate recovery of those critical business processes and systems identified by the business impact analysis, and (4) implement procedures for the ongoing maintenance of the business impact analysis and business recovery plan as well as comprehensive, routine (e.g., minimum once a year) testing of the plan. In addition, a full data center "power-down" test should be included in the business recovery plan. This report contained 19 recommendations overall to correct the internal control weaknesses and strengthen controls over House information resources. HIR fully concurred with the findings and recommendations and agreed to implement appropriate action to correct the deficiencies identified.

Relative to the telecommunications disaster recovery plan, the report noted the following: (1) no formal disaster recovery planning and testing existed for the telecommunications infrastructure, (2) redundant network telecommunications links are not in place for the House wide area network, (3) there is no physical off-site backup for the NCC, and (4) there is no backup connection for the existing T1⁹ line for the House connection to the Internet. The Exhibit on page 18 depicts the implementation status of contingency/disaster recovery recommendations related to telecommunications.

⁹ A telecommunications line which has a maximum operation speed of 1.4 million bits per second.

II. FINDINGS AND RECOMMENDATIONS

One of the objectives of this audit was to determine if emergency or contingency provisions have been incorporated into the major vendor contracts that support the House telecommunications network to ensure continuous vendor support is available and can be relied upon. Our review of the Communications Group's contract files indicated adequate coverage from a contractual viewpoint. A second objective involved the preparation of a limited HIR Communications organization and operations profile and a review of same for reasonableness. Based upon a review of available documentation and through discussions with Communications Group officials, we were satisfied as to the reasonableness of the organization structure and operations.

Finding A: Comprehensive, Proactive Approach Needed To Bolster Contingency And Disaster Recovery Planning

Since the House infrastructure places a high degree of reliance on the ability to communicate, the logical course of action would be to implement an approved and workable telecommunications contingency/disaster recovery plan designed to counter any number of disasters/threats in order to restore and maintain that capability. However, our review, indicated the Communications Group had not fully developed, completely documented, or tested an up-to-date, comprehensive contingency/disaster recovery plan. Without such a contingency/disaster recovery plan, HIR cannot ensure that Members, Committees, and other House offices would continue to have telecommunications services in the event of a disaster or that recovery would be timely and complete. The need to set a contingency plan in motion could occur at any time due to the potential threat of natural disaster, system or electrical failure resulting in some aspect of network failure, unintentional errors, terrorism, or other similar acts. Given the reactive nature/makeup of the existing plan, such unanticipated acts could seriously affect the House's ability to maintain telecommunications and continue business as usual.

The Communications Group relies on the presumption that there are too many disaster scenarios to deal with in a distributed network, therefore they contend it is more prudent to react to a disaster, assess its impact on the spot, and initiate a responsible recovery action. The Communications Disaster Recovery Plan in place has incorporated basic fundamentals for a disaster recovery plan but the plan lacks best industry standards necessary for complete, uninterrupted recovery. Internal control practices that are commonly accepted throughout the Federal government and private industry require the establishment of procedures to help protect critical files, programs, and system documentation from fire or other natural disasters. Further, these procedures should be formally documented, periodically updated and tested, and contain the detailed steps telecommunications support and operations personnel and the user community should take in the event of an emergency. Aside from the components of a Housewide contingency/disaster recovery plan (e.g., recovery teams, recovery action plan, vital records recovery, application systems operating procedures, system software configuration, data center equipment inventory, contingency plan testing, alternate processing facility, forms and supplies, plan maintenance, transportation and logistics, etc.), a distributed network can be recovered by

comprehensive documentation of telecommunications requirements, such as: (1) a comprehensive inventory of telecommunications equipment and software, (2) configuration, including switching equipment, multiplexors/concentrators, diagnostic devices, modems, telecommunications controllers, and telecommunications lines, (3) descriptions of speed, frequency, bandwidth, and circuit identification of telecommunications channels, (4) vendors and telephone company contacts, including telephone numbers and contracts, and (5) backup provisions, including contracts with the telephone company provider to automatically reroute lines on the basis of proper notification, location of company switching devices outside of the main facility, and switching facilities to an alternate site(s). Furthermore, disaster scenarios for distributed networks can be addressed in detail as we learned in discussions with officials in a large Executive Branch agency located not too far from the House (see below).

The Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Systems*, Appendix III.3.a.[3] mandates that "Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the

event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed." Although not required to follow OMB mandates, these requirements would serve the House well by providing generally accepted information systems guidance that is appropriate for any well-controlled computer and telecommunications facility. The contingency plan for the Communications Group should be established in conjunction with the House's overall contingency plan. The Communications Group contingency/disaster recovery plan cannot be adequately established without the implementation of the House-wide contingency plan to ensure that major telecommunications services required for the House to continue operations can be achieved. In the case of the House, it would be of paramount importance to have minimal business interruption and maximum telecommunications capabilities.

Telecommunications disaster recovery plan is inadequate

We reviewed the current telecommunications contingency/disaster recovery plan and discussed with the Communications Group management their philosophy of reacting to and devising an action plan after the disaster has occurred. Their reasoning for implementing a reactive plan versus a proactive plan was due to the seemingly endless number of scenarios that could effect a distributed network's operations. Consideration and action events would only be implemented for a disaster/disruption impact after a disaster has occurred. Then an assessment would be made and appropriate contingency/disaster recovery components would be implemented. In order to determine the level of difficulty involved in restoring a distributed network, we contacted a large Federal government agency (Agency) which has adequately implemented a mainframe and telecommunications contingency/disaster recovery plan. We discussed the sequence of events that took place in order for them to implement a telecommunications contingency/disaster recovery plan. They explained that limited resources forced them to look for a solution that would provide a comprehensive approach to all their needs, including telecommunications, but that required minimum investment in time and personnel. Agency officials utilized proprietary recovery software available off the GSA (General Services Administration) schedule to assist them in designing, implementing, and testing disaster recovery services for mainframe and telecommunications recovery. We obtained sample documentation to show the Communications Group management that at least one other Federal agency could document what and how their networking capabilities could be recovered, and explained the methodology that was used. Towards the end of our review, we were contacted by the HIR Security Manager to participate in a discussion about a comprehensive business recovery software (ironically, the same software that was used by our example agency) that may be under consideration for the House if budgetary resources are available. A meeting with the software vendor was held and as a result, their product has been added to HIR's audit action summary list to determine the feasibility of using it in the development of a comprehensive contingency/disaster recovery plan.

Furthermore, the concern that a natural disaster (i.e., fire, explosion, electrical failure, etc.) or other situation (such as a bomb threat, cable severing, wide area network failure, phone system failure, etc.) could occur that would limit or prevent access to the critical telecommunications areas had never been considered from a full or overlapping House-wide perspective. The potential that access to any telecommunications facility, data files, and equipment may be delayed or unavailable in the event of a business interruption needs to be considered. Without a well-designed and thoroughly tested contingency/disaster recovery plan in place, House telecommunication services and the Communications Group will be ill-prepared to minimize a system interruption in the event of a disaster. Failure to recover in a timely manner would significantly affect the communication services of House Members, Committees, and staff.

House-wide contingency/disaster recovery planning previously addressed

The comprehensive House audit performed during CY 1995 (see Prior Audit Coverage) contained specific recommendations to address the implementation of a comprehensive disaster recovery plan, including the development of procedures and identification and assignment of responsibilities. (The plan discussed in this report would be incorporated into the overall, House-wide contingency/disaster recovery plan.) The CAO responded to this recommendation, in part, by hiring a security manager for the House. The CAO further stated that business impact and cost analyses for various levels of disaster recovery protection would be prepared as part of the overall

security program and result in a proposal to the Committee on House Oversight as to alternatives and associated costs. Communications Group officials stated that they intend to use this analysis as the vehicle for identifying and developing a distributed network plan to assist in eliminating the weaknesses associated with the current telecommunications disaster recovery plan. (See Other Matters section for more on this issue.) Without the commitment of Member, Committee, House offices, and budgetary and staffing resources, the comprehensive disaster recovery plans needed for House-wide recovery may not occur. The loss of telecommunications services would substantially interrupt or prevent normal operations or create a potential shutdown of House operations.

Recommendations

We recommend that the Chief Administrative Officer:

1. Modify the current Telecommunications Contingency/Disaster Recovery Plan to encompass a proactive, detailed methodology that would encompass a distributed network topology and incorporate it into the overall, House-wide contingency/disaster recovery plan.
2. Given the current resource constraints, the Communications Group should assess the benefits to be derived from utilizing the capabilities of software-based development tools (executed by in-house staff or contractor) that would best meet the needs of the House for comprehensive telecommunications contingency/disaster recovery planning.
3. Implement formal telecommunications contingency/disaster recovery policies and procedures, routinely test the plan, and ensure that the plan is adequately maintained and updated on a regular basis.

Management Response

The Acting CAO concurred with the recommendations in this finding. In his January 16, 1997 response, the Acting CAO indicated HIR Communications and HIR Security will (1) secure the services of a qualified contractor to evaluate and upgrade the current contingency and disaster recovery plan, (2) assess and use, if applicable, software-based development tools to accomplish the planned upgrade, and (3) implement formal telecommunications policies and procedures governing the maintenance and routine testing of the plan. This effort will be a component of an overall, House-wide contingency/disaster recovery plan.

Office of Inspector General Comments

The planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding B: Tape Backup Storage and Rotation Procedures Need To Be Improved

Controls surrounding any thorough backup and recovery process require the availability of system software, application software, and data. During our review we noted deficiencies concerning the lack of off-site storage and rotation for the Private Branch Exchange (PBX) and telecommunications system backup tapes. Without an adequate off-site storage and rotation process, the House's ability to obtain backup data could be severely limited or restricted. As a result, the recovery process would not occur smoothly in order to minimize business interruption and reduce the risk of loss due to the unavailability of current data.

Internal control policies and procedures that are commonly accepted throughout the government and in private industry strongly recommend standard procedures be established for information technology operations covering significant software and tape backup. Furthermore, the rotation of these tapes to and from an off-site location increases the recovery factor by ensuring the most current software and data are in a location physically separate from the data center. HIR officials have not established and implemented adequate tape backup and off-site rotation procedures to minimize business interruptions and ensure a complete recovery. As a result, the inability to provide critical software and current data tapes may severely hamper the recovery process.

Telecommunications software/data and PBX system backup procedures need improvement

We reviewed the backup tape and off-site rotation procedures for the telecommunications system software (e.g., VTAM,¹⁰ NCP,¹¹ NetView,¹² etc.) with the Enterprise Computing (EC) group. A full volume backup is performed weekly which stores the system and application software and data to a storage tower located in the Library of Congress data center. The daily backups save incremental data for the telecommunications system and are stored onsite in the HIR central computer facility—they are not stored off-site in a secure location. The incremental tapes consist of seven days' worth of tapes that are used to backup the modifications to software from day-to-day. In the event of a disaster or business interruption, where access to the data center facility is unavailable, the House would have to locate the original input and re-create seven days worth of data.

Tapes from the PBX system configuration are run daily and weekly to backup the current feature set and specific terminal change and facilities management programs. Backup procedures are performed nightly and weekly for system configuration information in the event they are needed to recover from a major system failure. Furthermore, the tapes currently are not cycled out of the main switch room facility located in the Longworth Building to a secure location. This creates a vulnerability similar to the situation discussed above with telecommunications backup tapes. If access to the Longworth building is not available because of an emergency or disaster, all nightly and weekly system configuration information would be lost and have to be re-created.

Recommendations

We recommend that the Chief Administrative Officer:

1. Develop and implement routine procedures for off-site tape storage and retention of critical telecommunications software and data and incorporate these procedures into the telecommunications contingency/disaster recovery plan.
2. Modify existing procedures to ensure that backup tapes for PBX system processes and for telecommunications system software are rotated off-site to a secure location.

Management Response

¹⁰ VTAM (Virtual Telecommunications Access Method) is a set of programs that control communications between terminals and application programs.

¹¹ NCP (Network Control Program) is a program that manages the top of an SNA domain, usually on a mainframe.

¹² An IBM licensed program used to monitor a network, manage it, and diagnose network problems.

The Acting CAO concurred with the recommendations in this finding. Existing procedures for off-site tape storage and retention of critical telecommunications software were updated on December 1, 1996 to include all daily backups for critical libraries associated with telecommunications software. The new procedures were incorporated into the current plan on December 27, 1996. Similar changes were made on December 27, 1996 to existing procedures to include storage and rotation of weekly PBX and telecommunications system software backup tapes. These procedures will be incorporated into the current plan by January 30, 1997.

Office of Inspector General Comments

The planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding C: Centralized PBX Platforms Place House-wide Telephone Services At Risk

The placement of the existing voice system architecture increases the vulnerability of outages for major portions of telephone service at the House. All four PBX platforms serving House Members and staff are located in the Longworth building switch room. Because of the centralized placement of these PBX platforms, there is a greater potential for a single event (mechanical, natural or man-made disaster) to disrupt telephone service for all or a major portion of the House's telephone users. We could not determine why business continuity or disaster preparedness issues were not considered in the placement of these platforms, however Communications Group officials indicated the voice system architecture currently in place was originally designed primarily with operational and economic benefits in mind.

Federal government and private industry contingency guidelines and practices are well established

Federal government and private industry standards and practices call for the establishment of standards, policies, and procedures for contingency planning and backup and recovery, including the periodic testing of plans of essential operations, and that such practices be a part of an agency's IRM (Information Resources Management) and strategic plans. Disaster recovery plans should anticipate potential, critical business interruptions and disaster or emergency scenarios and cover all significant processes and operations, including telecommunications alternatives, to limit any adverse impact to an agency's operations. The periodic testing of such plans would minimize the adverse impact to operations and confirm the viability of such plans.

Voice system architecture vulnerabilities need to be addressed

The PBX platforms located in the Longworth office building support approximately 20,000 lines, including voice, fax and modem, to House users. These systems support remote modules serving other House buildings and are interconnected to the main system through proprietary links that run through secure tunnels. These tunnels house various cables and wiring, such as telecommunications and electrical cables, and access to tunnels is controlled by the Architect of the Capitol. The unavailability of the main switching platforms or any one of the proprietary links will result in a significant loss of telephone service.

The existing voice services are distributed between four main switching platforms co-located in the basement of the Longworth building. These systems are in the process of being further consolidated into two voice switching platforms in the near term. While the main systems are configured with redundant, critical components and battery backup to reduce the potential for failure, further consolidation increases the risk and the accompanying impact of an outage if a system failure were to occur. The remote modules serve the Cannon, Capitol, and Annex buildings which are connected to the main system via proprietary links that enable the remote modules to process calls. Remote modules provide the minimum of intelligence and require the main system processors in the Longworth building to set up, retain, and tear down calls. If the links are not operational, telephone service at the remote sites will be completely disrupted until the link is re-established.

We raised this issue with Communications Group officials who responded that the cost to install redundant PBX platforms at other locations at this time would be extremely costly, but they did not provide any firm figures or reference a cost-benefit analysis to support such a statement. We agree that installing redundant PBXs would involve a cost but we do not know what those costs are nor do we know what the risk factor is if nothing is done and neither does the Communications Group. The unavailability of cost figures or a cost-benefit analysis to support management's position is further compounded by the absence of a formal contingency risk assessment. A risk assessment would provide senior management with an evaluation of the risks related to the contingency and how the Communications Group has addressed those risks. Successful implementation of a risk assessment process can and often does involve the use of risk management, a process of identifying risks, risk-reducing measures, and the budgetary affect of implementing decisions related to the acceptance, avoidance, or transfer of risk. The final phase of risk management includes the process of assigning priorities, and, budgeting, implementing, and maintaining appropriate risk-reducing measures in a continuous or periodic cycle of assessment, analysis, and management or administrative action. Without knowing the specific risks or exposures associated with a particular management decision, for example, the concentrated placement of PBX platforms in one location, management will be ill-prepared to deal with such a contingency should a disaster strike that

operation. It is also common but incorrectly assumed that risk management is concerned only with catastrophic threats, that it is related only to contingency planning. A well-conceived and well-executed risk assessment can also effectively identify and quantify the consequences of a wide array of threats that can and do occur as a result of ineffectively implemented or nonexistent management or operational controls. Risk assessment can be a useful management tool for identifying an optimal, cost-effective mix of management, operational, and environmental controls. An informed manager will have evaluated the risks and base his/her decision on the data or facts that came out of a risk assessment and have some basis for having taken management's current position.

Recommendations

We recommend that the Chief Administrative Officer:

1. Conduct a contingency-based risk assessment, including threat and vulnerability analyses, of the PBX platforms located in the Longworth building.
2. Use the results of the risk assessment to determine the appropriate course of action, which would involve:
 - (a) taking no action at all, formally documenting the level of risk as being acceptable, or
 - (b) conducting a cost-benefit analysis to determine the most cost-effective mix of risk reduction measures to implement, and then implementing them.
3. Modify the current HIR House-wide contingency plan to add the PBX platforms and include them in cyclical testing.

Management Response

The Acting CAO concurred with the recommendations in this finding. The Acting CAO indicated HIR Communications and HIR Security will (1) utilize a contractor to assess the threat and vulnerability potential to the PBX platforms in the Longworth building; (2) use the results of that assessment to (a) do nothing—noting the risk is acceptable or (b) initiate a contractor-run cost/benefit analysis to implement risk reduction measures; and (3) include the PBX platforms and cyclical testing of same in the upgraded contingency and disaster recovery plan. It is anticipated that these actions can be fully implemented by the end of Fiscal Year 1998.

Office of Inspector General Comments

The planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding D: Potential Hazards Could be Eliminated With Improvements To The Current Wiring Infrastructure

During our review we noted conditions with regard to the current wiring infrastructure that are potentially hazardous and which, in our view, require management attention. Specifically, we found that, in some instances, cables are not adequately protected; telecommunications vendor spaces and wire closets have environmental and safety hazards; and the telecommunications equipment rooms throughout the House facilities, in particular, the main switch room at the Longworth Building, present major security concerns. It is also our opinion that changes to documentation methods for existing telecommunication circuits would benefit current and future maintenance efforts. The wiring infrastructure throughout the House office buildings is one the most critical components of the House Telecommunications network. This infrastructure carries all voice, data, and video traffic. Correct installation and maintenance is crucial to maintaining the integrity of House telecommunications services. These conditions primarily result from inadequate written policies and procedures related to the wiring infrastructure.

Telecommunications room security

Critical telecommunications wire closets (closets with equipment and/or cable cross-connect hardware) were accessible by audit staff without escort. Further, it is our understanding that access and use of these rooms is not the sole jurisdiction of HIR. Thus, HIR's lack of responsibility for all telecommunications areas, coupled with the ease of access to these rooms, causes serious concerns for the security of information in the House.

Poor "housekeeping" in demarcation¹³ rooms

Poor "housekeeping" habits (i.e., cigarette butts and trash on floors, scrap wire bags filled to overflowing, empty equipment boxes, large amounts of abandoned cross connect wires, etc.) were noted in telecommunications demarcation rooms (primarily in the Longworth, U.S. Capitol, and Annex II). In addition, we noted a few of the larger wire closet areas are currently being utilized as storage areas, while boxes of excess materials, discarded furniture, and other items are maintained in these spaces. These situations present potential problems such as possible fire hazards and unsafe conditions for personnel, not to mention that it presents a generally unprofessional working environment. When we discussed this matter with Communications Group officials, they explained that wire closets are taken care of under a commercial cleaning contract (which is currently being re-competed) but that the demarcation rooms, which are controlled by the Architect of the Capitol (AOC), are not included in that contract. Also, with the abandoned cross connects, a situation exists where potential contact with other working circuits could cause undesirable effects (i.e., noise on voice circuits, total outages due to shorted pairs, etc.).

In addition, we encountered what we would describe as undesirable temperature conditions during our visits to the demarcation room in Annex II, which contains a fiber optic multiplexer. Even though we did not use temperature measuring equipment, we felt the room was unusually hot with no noticeable movement of air or air conditioning present—a condition that may adversely affect the performance or capabilities of the equipment. During our exit discussion with Communication Group officials, they explained that the temperature in that room is normally maintained at a rate within acceptable ranges specified by the manufacturer and that it is monitored regularly by a House engineer. Further, while the tolerances as specified for a particular piece of equipment may not be exceeded, the temperature range for an equipment room should be appropriate for long term operation of electronics by various manufacturers. The EIA/TAI 569 has stringent equipment room specifications that could be used as a guideline for HIR in this regard. It is imperative to provide a safe and productive working environment for all personnel as well as all equipment expected to operate in the affected areas. The detrimental effect that these environmental concerns can have on electronic equipment can not be overemphasized. As the heat and humidity rise, so does the bit error rate of equipment which supports the network as does the general failure rate of telecommunications electronics. Given the apparent differences with regard to our observations and the

¹³ A demarcation room is the area in a building in which the carrier facilities are handed off to the user organization. This location is the demarcation between the outside plant of the carrier, which is the carrier's responsibility, and the inside wiring of the building, which is the responsibility of the landlord/owner.

Communications Group's claims, the obvious solution would entail some form of short-term monitoring to determine if this is a problem. A condition that complicates this situation, according to Communications Group officials, is the fact that while the demarcation room houses telecommunications equipment and cabling, the room itself is under control of the AOC. Any changes that may need to be made in that room will require agreement and coordination between the CAO and the AOC.

A single fiber path to the main switch room presents disaster recovery concerns

Best practices within a low tolerance environment like the House require a diverse protection scheme for voice services that would minimize unanticipated interruptions to the end user. A diverse protection scheme (in this case, a diverse path) is a network design technique which implements redundant connections between two points (e.g., switches) that are diversely routed to protect against catastrophic failures. The loss of one connection due to physical damage of property, etc. will be transparent to users as the other, diverse connection remains to provide service. An alternative method, such as a sheath diversity protection scheme, may be considered where impediments such as physical or budgetary constraints exist. This particular scheme involves separating the lines going between two locations into different groups of cables and housing the cables in the same conduit.

The main switch room at the Longworth Building directly supports voice services to the Longworth and Rayburn Buildings. This switch also supports five optic remote sites, specifically, Annex I (O'Neil Building), Annex II (Ford Building), the Cannon Building, the U.S. Capitol, and 501 First Street, by way of fiber optic cable. According to HIR, the spaces in which these fiber optic cables have been installed are considered secure spaces. Further, they stated that these fiber optic cables never leave the House Campus and are under the control of the U.S. Capitol Police. However, HIR has little control over the myriad of unexpected circumstances that could arise affecting their customers' voice services. For example, the possibility exists, with the many ongoing renovations, that damage to a single fiber cable could isolate one or more of the remote sites. Thus, the House should assess the benefits to be derived from adopting a totally diverse protection scheme for voice services whenever possible. This scheme would, ideally, provide a second cable connection for services in case the primary cable connection was damaged.

Also, the House needs to review its policies with regard to the use of plastic innerduct for fiber cable runs. Wherever possible, the House should identify cable paths that utilize innerduct and assess both the risks and costs associated with replacing them with rigid conduit. Rigid conduits would ensure maximum protection for critical fiber cables and provide significantly better protection than innerduct conduit. Communications Group officials explained that the majority of innerduct runs exist in the Capitol building, which is under the jurisdiction of the AOC and whose policy it is to use innerduct conduit. These officials agreed on the merits of using rigid conduit but raised the issue of jurisdiction and questioned whether the costs associated with replacing existing innerduct runs could be justified.

Recommendations

We recommend that the Chief Administrative Officer:

1. Modify the current room cleaning contract to include the House's demarcation rooms.
2. Develop and/or review contract monitoring procedures to ensure that (a) a monitor is designated to oversee the contract, (b) agreed upon work is being completed and rooms are being cleaned; (c) random inspections are conducted to determine contract compliance; and (d) appropriate, corrective action is taken for non-compliance.
3. Request the Architect of the Capitol review procedures for monitoring temperature readings within the demarcation rooms. If procedures already exist, review them for compliance to determine if the facts presented in this report were anomalous or occur routinely.
4. Initiate deliberations with the Architect of the Capitol regarding the feasibility of transferring responsibility for the demarcation room to the HIR Communications Group,

and evaluate points of responsibility for all demarcation rooms as well as procedures governing access to these areas.

5. Conduct a risk assessment and/or benefit-cost analysis to determine the viability of adopting a diverse path protection scheme for voice services.
6. Develop Communications' policy that establishes rigid conduit as a de facto standard with justified exceptions made for the use of innerduct conduit.

Management Response

The Acting CAO concurred with the recommendations in this finding. The Acting CAO indicated that HIR Communications will (1) incorporate changes into the new cleaning contract to include the demarcation room; (2) develop appropriate oversight procedures to ensure cleaning contract requirements are being met; (3) request the AOC review procedures for monitoring temperatures within demarcation rooms; (4a) negotiate with the AOC to transfer responsibility for the demarcation rooms to HIR Communications; (4b) work with HIR security to develop procedures governing access to demarcation rooms; (5) utilize a contractor to assess the viability of adopting a diverse path protection scheme for voice services; and (6) develop written policies establishing rigid conduit as the de facto standard with justified exceptions made for the use of innerduct conduit. Corrective action on items 1, 2, 3, 4a, and 6 will be completed and/or fully implemented by January 31, 1997. Security access procedures (item 4b) will be implemented by May 1, 1997 and action on item 5 will be fully implemented by the end of Fiscal Year 1998.

Office of Inspector General Comments

The planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Status Of Implementation Of Prior Telecommunications Audit Report Recommendations

EXHIBIT


Audit Report/Recommendations	Implementation Status	Comments on Corrective Actions Taken And/Or Planned	Scheduled Date of Completion
Audit Report No. 95-CAO-18, entitled <i>House Computer Systems Were Vulnerable To Unauthorized Access, Modification, And Destruction</i>, dated July 18, 1995:			
B.1. Implement a comprehensive disaster recovery plan that outlines specific disaster recovery procedures and responsibilities for both HIR operations (including the identification and coordination of a backup arrangement for the Network Control Center), and office-level systems.	Partially Implemented	A formal business recovery plan for telecommunications now exists (but is taken to task in Finding A). A contract will be let to update the current telecommunications plan which will be rolled into a House-wide contingency/disaster recovery plan. Backup arrangements for the NCC have been completed and minor environmental issues remain before the site can be tested.	Plan Sept. 1998 Backup NCC June 1997
B.2. Implement and update the business impact analysis identifying those business processes and systems that are critical to the business continuity of the organizations supported by HIR, as well as office-level systems and telecommunications links supporting Member, Committee, and other House operations currently not addressed by the existing mainframe data center disaster recovery plan.	Partially Implemented	A second TCP/IP interface to the mainframe was installed in October 1996. The redundancy issue regarding the PVCs will need to be evaluated because it entails costs that will have an impact on this decision. Redundant PVCs were implemented and tested at one point in the life of the network but were backed off due to problems related to dynamic routing protocols used on the network. Those problems are now believed to have been addressed and, once the current expansion of the frame relay network has been completed, redundant PVCs will be implemented, if they are cost-effective.	Redundant PVCs Pending - No date scheduled
B.3. Evaluate backup and business recovery alternatives that would facilitate recovery of those critical business processes and systems identified by the business impact analysis and select the most appropriate alternative.	Not Implemented	With regard to these issues in general, Communications Group officials indicated they would work them into the business impact analysis that is under development and soon to be addressed by the HIR Security Manager. The results of the impact analysis should give them better information to set priorities and address the redundancy issues raised in this audit.	Sept. 1998

Audit Report/Recommendations	Implementation Status	Comments on Corrective Actions Taken And/Or Planned	Scheduled Date of Completion
Audit Report No. 95-CAO-18, entitled <i>House Computer Systems Were Vulnerable To Unauthorized Access, Modification, And Destruction</i>, dated July 18, 1995:			
B.4. Implement procedures for the ongoing maintenance of the business impact analysis and business recovery plan as well as comprehensive, routine (e.g., minimum once a year) testing of the plan. Additionally, a full data center "power down" test should be included in the business recovery plan.	Not Implemented	Procedures are under development and will be addressed by the HIR Security Manager as part of the overall, House-wide contingency and disaster recovery plan.	Sept. 1998

**Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515**

Memorandum

To: Robert B. Frey III
Deputy Inspector General

From: Jeff Trandahl 
Acting Chief Administrative Officer

Subject: Contingency and Disaster Recovery Planning Audit

Date: JAN 16 1997

Thank you for the opportunity to comment on the draft audit report. We have carefully reviewed the draft audit report and the recommendations contained therein and are in general agreement. Several of the responses state the intention to hire a contractor to provide services to HIR. It is anticipated that to the extent feasible and legally permissible, all of the work will be done by a single contractor. Where different specific analytical skills are required, the contractor will be allowed to subcontract with others who possess the necessary skills and experience. Specific comments on each recommendation follow.

Finding A: Comprehensive, Proactive Approach Needed to Bolster Contingency and Disaster Recovery Planning

Recommendations:

We recommend that the Chief Administrative Officer:

1. Modify the current Telecommunications Contingency/Disaster Recovery Plan to encompass a proactive, detailed methodology that would encompass a distributed network topology and incorporate it into the overall, House-wide contingency/disaster recovery plan.
2. Given the current resource constraints, the Communications Group should assess the benefits to be derived from utilizing the capabilities of software-based development tools (executed by in-house staff or contractor) that would best meet the needs of the House for comprehensive telecommunications contingency/disaster recovery planning.
3. Implement formal telecommunications contingency/disaster recovery policies and

procedures, routinely test the plan, and ensure that the plan is adequately maintained and updated on a regular basis.

CAO/HIR Response: Concur

Recommendation 1.

HIR Communications and HIR Security will utilize the House of Representatives' *Guidelines for the Procurement of Goods and Services* to hire a contractor to conduct a telecommunications risk assessment and modify the current Telecommunications Contingency/Disaster Recovery Plan to encompass a proactive, detailed methodology that would encompass the House's distributed network topology. This effort will be a component of an overall, House-wide contingency/disaster recovery plan. Fiscal Year 1997 funds are available for this purpose. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Recommendation 2.

HIR Communications and HIR Security will utilize the House of Representatives' *Guidelines for the Procurement of Goods and Services* to hire a contractor to conduct a telecommunications risk assessment and modify the current Telecommunications Contingency/Disaster Recovery Plan. This effort will include assessing the benefits to be derived from utilizing the capabilities of software-based development tools (executed by in-house staff or contractor). Fiscal Year 1997 funds are available for this purpose. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Recommendation 3.

Once Recommendations 1 and 2 above have been implemented, HIR Communications will Implement formal telecommunications contingency/disaster recovery policies and procedures, routinely test the plan, and ensure that the plan is adequately maintained and updated on a regular basis. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Finding B: Tape Backup Storage and Rotation Procedures Need to be Improved.

Recommendations:

We recommend that the Chief Administrative Officer:

1. Develop and implement routine procedures for off-site tape storage and retention of critical telecommunications software and data and incorporate these procedures into the telecommunications contingency/disaster recovery plan.

2. **Modify existing procedures to ensure that backup tapes for PBX system processes and for telecommunications system software are rotated off-site to a secure location.**

CAO/HIR Response: Concur

Recommendation 1.

Routine procedures exist for off-site tape storage and retention of critical telecommunications software and data. Daily and weekly backups for critical telecommunications software such as VTAM and NCP are generated. A majority of daily backups and all weekly backups are stored off-site at the Library of Congress. Existing procedures were updated on December 1, 1996 to include the off-site storage of all daily backups for critical libraries associated with telecommunications software such as VTAM and NCP. The new procedure(s) were incorporated into the telecommunications contingency/disaster recovery plan on December 27, 1996.

Recommendation 2.

Procedures currently exist for off-site storage of back-up tapes at a secure location. Those procedures will be modified to include the storage and rotation of the weekly PBX and telecommunications system software back-up tapes. Modifications to the existing procedures were made on December 27, 1996, and will be incorporated into the telecommunications contingency/disaster recovery plan by January 30, 1997.

Finding C: Centralized PBX Platforms Place House-wide Telephone Services at Risk

Recommendations: We recommend that the Chief Administrative Officer:

1. **Conduct a contingency-based risk assessment, including threat and vulnerability analyses, of the PBX platforms located in the Longworth Building.**
2. **Use the results of the risk assessment to determine the appropriate course of action, which would involve:**
 - (a) **taking no action at all, formally documenting the level of risk as being acceptable, or**
 - (b) **conducting a cost-benefit analysis to determine the most cost-effective mix of risk reduction measures to implement, and then implementing them.**
3. **Modify the current HIR House-wide contingency plan to add the PBX platforms and include them in cyclical testing.**

CAO/HIR Response: Concur

Recommendation 1.

HIR Communications and HIR Security will utilize the House of Representatives' *Guidelines for the Procurement of Goods and Services* to hire a contractor to conduct a telecommunications risk assessment, including threat and vulnerability analyses, of the PBX platforms located in the Longworth Building. This effort will be a component of an overall, House-wide contingency/disaster recovery plan. Fiscal Year 1997 funds are available for this purpose. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Recommendation 2.

HIR Communications and HIR Security will evaluate the telecommunications risk assessment to determine the level of risk. If the level of risk is not acceptable, then HIR will conduct a cost-benefit analysis to determine the most cost-effective mix of risk reduction measures to implement, and then implement them. This effort will be a component of an overall, House-wide contingency/disaster recovery plan. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Recommendation 3.

HIR Communications and HIR Security will utilize the House of Representatives' *Guidelines for the Procurement of Goods and Services* to hire a contractor to conduct a telecommunications risk assessment. This effort will include modifying the current HIR House-wide contingency plan to add the PBX platforms and include them in cyclical testing. Fiscal Year 1997 funds are available for this purpose. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Finding D: Potential Hazards Could be Eliminated with Improvements Over the Current Wiring Infrastructure.

Recommendations:

We recommend that the Chief Administrative Officer:

1. Modify the current room cleaning contract to include the House's demarcation rooms.
2. Develop and/or review contract monitoring procedures to ensure that (a) a monitor is designated to oversee the contract, (b) agreed upon work is being completed and rooms are being cleaned; (c) random inspections are conducted to determine contract compliance; and (d) appropriate, corrective action is taken for non-compliance.
3. Request the Architect of the Capitol review procedures for monitoring temperature readings within the demarcation rooms. If procedures already exist, review them for compliance to determine if the facts presented in this report were anomalous or occur

routinely.

4. Initiate deliberation with the Architect of the Capitol regarding the feasibility of transferring responsibility for the demarcation rooms to the HIR Communications Group, and evaluate points of responsibility for all demarcation rooms as well as procedures governing access to these areas.
5. Conduct a risk assessment and/or benefit-cost analysis to determine the viability of adopting a diverse path protection scheme for voice services.
6. Develop Communications' policy that establishes rigid conduit as a de facto standard with justified exceptions made for the use of innerduct conduit.

CAO/HIR Response: Concur

Recommendation 1.

HIR Communications has developed a Scope of Work for potential bidders that includes the cleaning of the House's demarcation rooms. Once bids are received, a purchase order will be generated to the vendor offering the House the best value. The terms and conditions of this procurement will include the cleaning of the demarcation rooms. This recommendation will be fully implemented by January 31, 1997.

Recommendation 2.

In conjunction with establishing a new vendor agreement for the cleaning of telecommunications facilities, HIR Communications will fully document contract monitoring procedures to ensure that (a) a monitor is designated to oversee the contract, (b) agreed upon work is being completed and rooms are being cleaned; (c) random inspections are conducted to determine contract compliance; and (d) appropriate, corrective action is taken for non-compliance. This recommendation will be fully implemented by January 31, 1997.

Recommendation 3.

HIR Communications will request that the Architect of the Capitol review procedures for monitoring temperature readings within the demarcation rooms. This request will be fully documented in writing. This recommendation will be fully implemented by January 31, 1997.

Recommendation 4.

HIR Communications will request that the Architect of the Capitol transfer responsibility for the demarcation rooms to the HIR Communications Group. This request will be fully documented in writing and will be fully implemented by January 31, 1997.

HIR Communications will work with HIR Security to develop procedures governing access to the demarcation rooms. These procedures will be part of a comprehensive program for access management for all telecommunications facilities. These will be fully documented and implemented by May 1, 1997.

Recommendation 5.

HIR Communications and HIR Security will utilize the House of Representatives' *Guidelines for the Procurement of Goods and Services* to hire a contractor to conduct a telecommunications risk assessment including analysis to determine the viability of adopting a diverse path protection scheme for voice services. This effort will be a component of an overall, House-wide contingency/disaster recovery plan. Fiscal Year 1997 funds are available for this purpose. It is anticipated that this recommendation can be fully implemented by the end of Fiscal Year 1998.

Recommendation 6.

HIR Communications will develop written policy that establishes rigid conduit as a de facto standard with justified exceptions made for the use of innerduct conduit. This will be completed by January 31, 1997.